



## Common Criteria

Ms. Jean Schaffer  
NIAP Director  
(410) 854-4458

Mr. Ken Elliott  
Senior Validator  
(410) 312-1405

# Agenda

- Overview: NIAP and CCEVS
- Governing Policies
- CC Introduction and General Model
- Security Functional Requirements
- Security Assurance Requirements
- U.S. Government Protection Profiles
- Contact Information

# Overview: NIAP and CCEVS

# Today's Challenge

- Consumers have access to an increasing number of security-enhanced IT products with different capabilities and limitations
- Consumers must decide which products provide an appropriate degree of protection for their information systems
- *Impact: Choice of products affects the security of systems in the critical information infrastructure*

# The Fundamentals

Building more secure systems depends on the use of---

- Well defined IT security requirements and security specifications
  - *describing what types of security features we want...*
- Quality security metrics and appropriate testing, evaluation, and assessment procedures
  - *providing assurance we received what we asked for...*

# Introducing NIAP

- The National Information Assurance Partnership (NIAP) is a U.S. Government initiative designed to meet the security testing, evaluation, and assessment needs of both information technology (IT) producers and consumers
- NIAP is a collaboration between the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) in fulfilling their respective responsibilities under the Computer Security Act of 1987

# NIAP Program Areas

- Security Requirements Definition and Specification

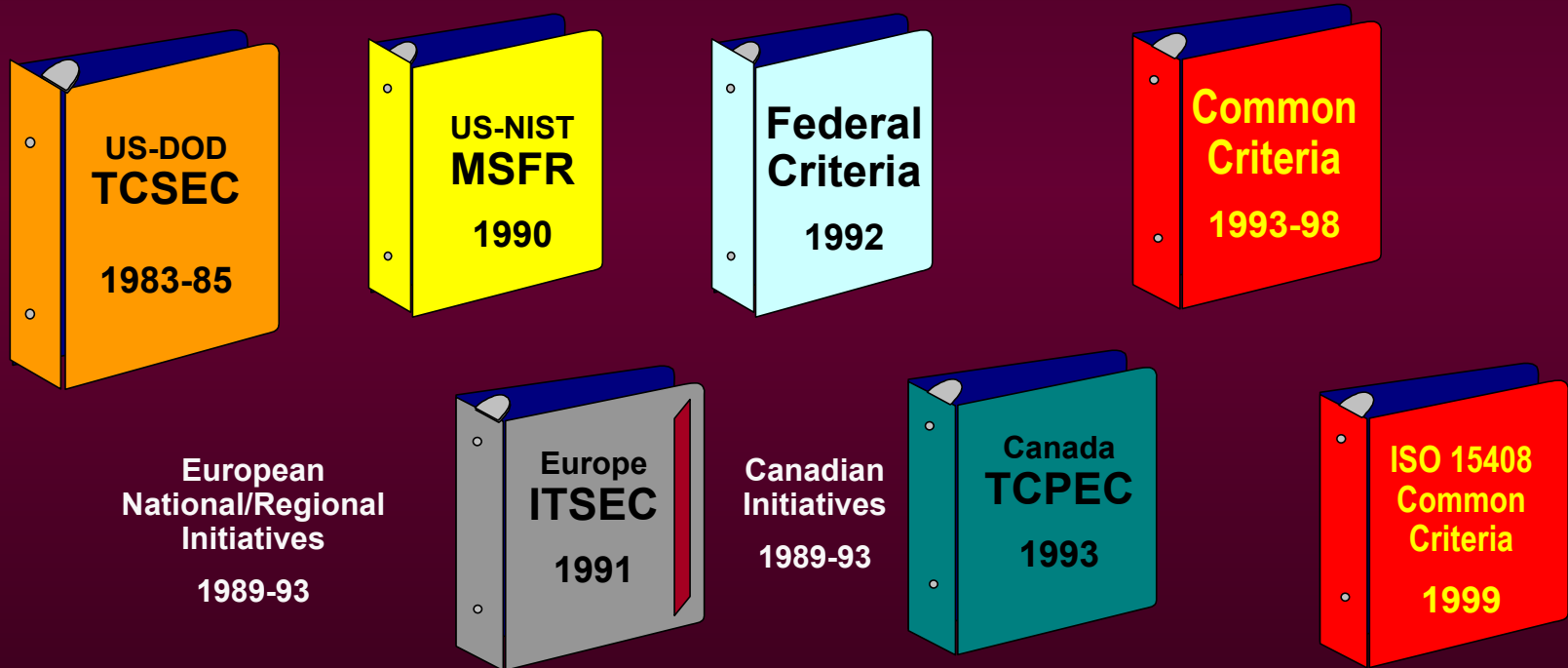
*How do we tell product and systems developers what types of IT security we want?*

- Product and System Security Testing, Evaluation, and Assessment

*How do we know if developers produced what we asked for?*

# An Evolutionary Process

Two decades of research and development...





# Common Criteria: The International Standard

## *What the standard is –*

- Common structure and language for expressing product/system IT security requirements (Part 1)
- Catalog of standardized IT security requirement components and packages (Parts 2 and 3)

## *How the standard is used –*

- Develop protection profiles and security targets -- specific IT security requirements and specifications for products and systems
- Evaluate products and systems against known and understood IT security requirements

# Mutual Recognition Arrangement

NIAP, in conjunction with the U.S. State Department, negotiated a Common Criteria Recognition Arrangement that:

- Provides recognition of Common Criteria certificates among 18 nations
- Eliminates need for costly security evaluations in more than one country
- Offers excellent global market opportunities for U.S. IT industry



®

# Common Criteria Mutual Recognition Arrangement



US



Canada



UK



Germany



France

**Certificate  
Producers**



Japan



Australia/New Zealand



Netherlands



Finland



Greece



Italy



Norway



Spain



Israel



Sweden



Austria



Turkey



Hungary

**Certificate  
Consumers**

National Information Assurance Partnership®

# Common Criteria Evaluation and Validation Scheme (CCEVS)

- **Evaluates conformance of the security features of IT products to the *International Common Criteria (CC) for Information Technology Security Evaluation*.**
- **Issues Certificates to vendors for successful completion of evaluations.**
  - Not an NSA or NIST endorsement
  - Not a statement about goodness of product

	<b>National Information Assurance Partnership</b>	
	<b>Common Criteria Certificate</b>	
	<b>Vendor Name</b>	
	<p>The IT product identified in this certificate has been evaluated at an accredited testing laboratory using the Common Methodology for IT Security Evaluation (Version X) for conformance to the Common Criteria for IT Security Evaluation (Version X). This certificate applies only to the specific version and release of the product in its evaluated configuration. The product's functional and assurance security specifications are contained in its security target. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by any agency of the U.S. Government and no warranty of the IT product is either expressed or implied.</p>	
Product Name:	Name of CCTL:	
Version and Release Numbers:	Validation Report Number:	
Protection Profile Identifier:	Date Issued:	
Evaluation Platform:	Assurance Level:	
<hr/>		
Director, Common Criteria Evaluation and Validation Scheme National Information Assurance Partnership		Information Assurance Director National Security Agency

# CCEVS Information

## <http://niap.nist.gov/cc-scheme>





[NIAP Home](#)
[CCEVS Home](#)
[About Us](#)
[Contact Us](#)
[Help](#)
[Site Map](#)
Jan 13, 2004

**Search NIAP CCEVS**

**The Big CCEVS Picture**

- Defining the CCEVS
- CCEVS Objectives
- Eval/Validation Primer
- CCEVS Validation Body
- Historical Perspective
- Guidance to Consumers
- CC Testing Labs
- CCRA & Partners
- Acronyms & Terms
- Upcoming Events
- The OR/OD Process
- What's New

**CCEVS Products**

- Validated Products List
- Validated Protection Profiles
- Products in Evaluation
- PPs in Development
- Archived Validated Products

**Docs & Guidance**

- FAQs
- Scheme Policy Letters
- Scheme Publications
- CC Documentation
- CEM Documentation
- Forms

**Click here >>>**

**NSTISSP No. 11, Revised Fact Sheet**  
**National Information Assurance Acquisition Policy**  
**(Includes deferred compliance guidelines and procedures)**  
**July 2003**



Available products to assist in making a more secure infrastructure.



Boosting consumer confidence through evaluation and testing of vendor products.



Policy that influences our adherence to the Common Criteria.

- ▶ VPL (by Product Type)
- ▶ VPL (by Assurance Level)
- ▶ VPL (by Product Name)
- ▶ VPL (by Vendor)
- ▶ Archived Evaluated Products
- ▶ Products in Evaluation
- ▶ Validated Protection Profiles
- ▶ PPs in Development

- ▶ Getting a Product Evaluated
- ▶ Finding a CCTL
- ▶ Getting a CCTL Accredited

- ▶ DOD Directive #8500.1
- ▶ DOD Instruction #8500.2
- ▶ NSTISSP No. 11, Revised Fact Sheet (July 2003) **NEW**
- ▶ NSTISSP No. 11 Fact Sheet (Jan 2000)
- ▶ NIST Spec Pub 800-23
- ▶ NSD 42
- ▶ NSTISSAM Compusec/1-99
- ▶ USAF CIO Memorandum
- ▶ Pres. Decision Directive 63
- ▶ For a comprehensive listing other pertinent IA-related docs, [Click Here.](#)

# U.S. Approved Common Criteria Testing Laboratories

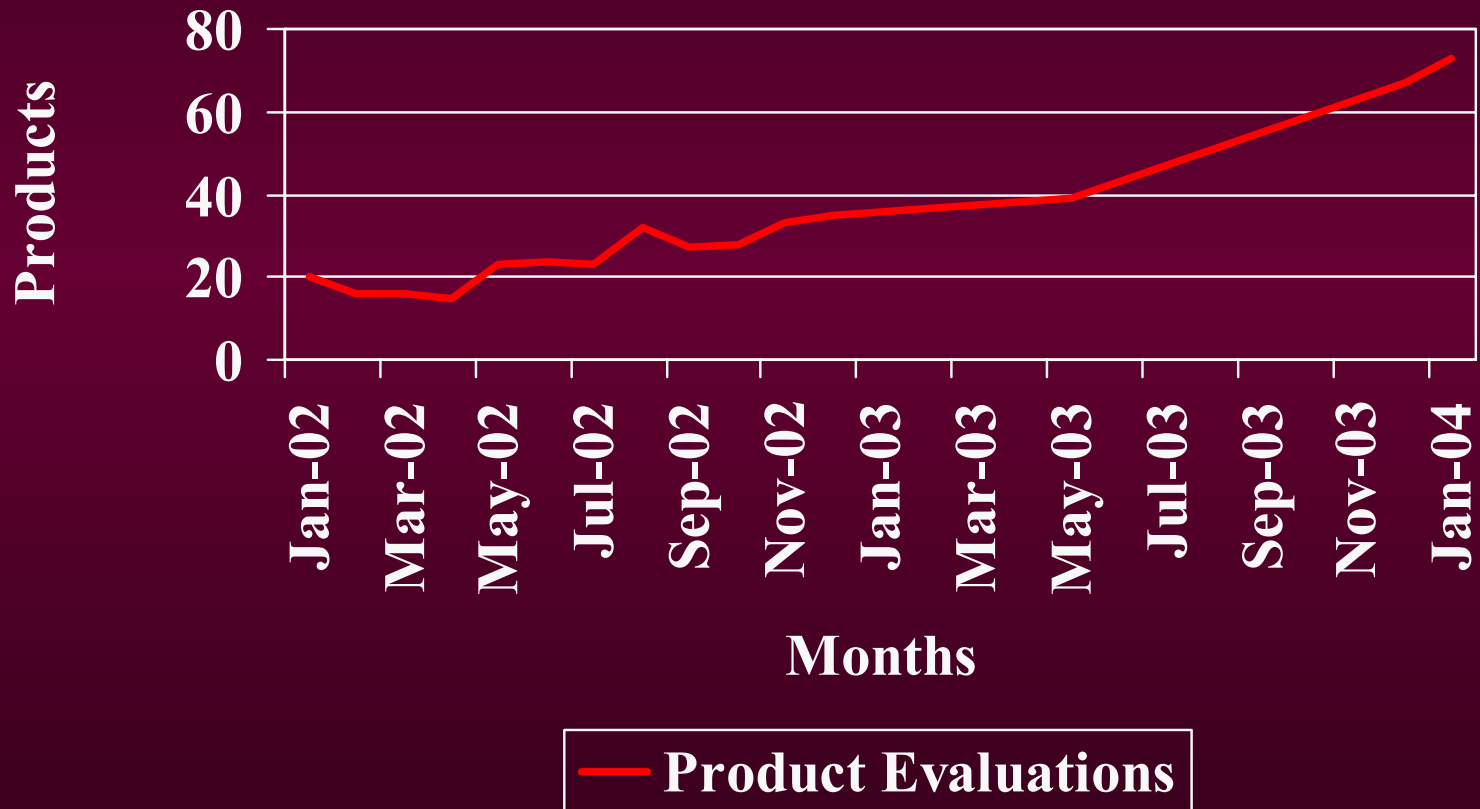
- |    |   |                                |
|----|---|--------------------------------|
| 1. | <b>Booz, Allen &amp; Hamilton</b>       | <b>Linthicum, Maryland</b>     |
| 2. | <b>Cable &amp; Wireless</b>             | <b>Sterling, Virginia</b>      |
| 3. | <b>COACT, Inc.</b>                      | <b>Columbia, Maryland</b>      |
| 4. | <b>Computer Sciences Corp.</b>          | <b>Annapolis Junction, MD</b>  |
| 5. | <b>Criterion Independent Labs</b>       | <b>Fairmont, West Virginia</b> |
| 6. | <b>Cygnacom Solutions, Inc.</b>         | <b>McLean, Virginia</b>        |
| 7. | <b>InfoGard Laboratories, Inc</b>       | <b>San Luis Obispo, CA</b>     |
| 8. | <b>Science Applications Int'l Corp.</b> | <b>Columbia, MD</b>            |
| 9. | <b>..... More Applicants Received</b>   |                                |

# NIAP CCEVS Project Status

- As of January 2004
  - 73 products “in progress” (70 STs, 3 PPs)
  - 53 certificates issued to date (36 STs, 17 PPs)
  - 16 cancelled/withdrew

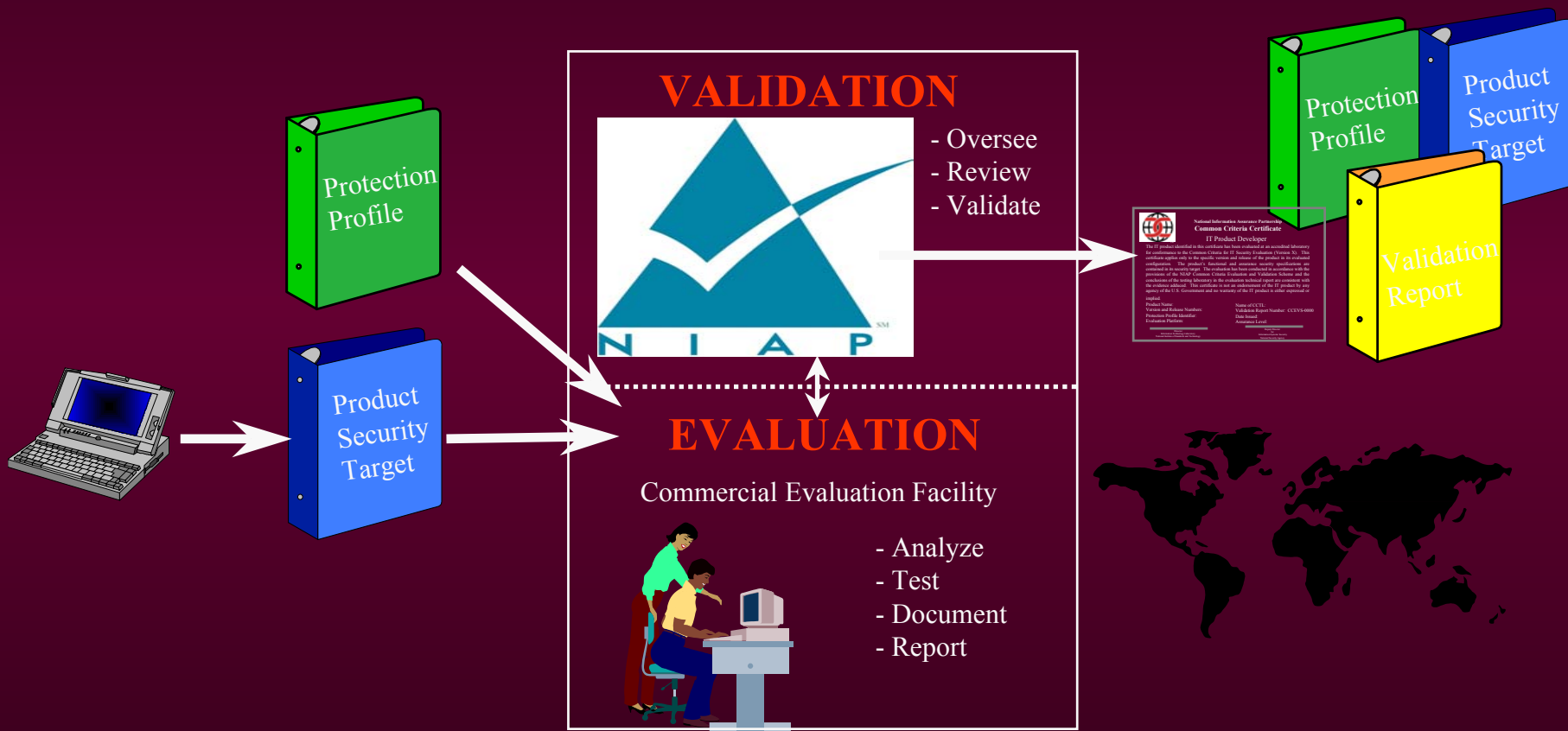
# 2002- 2003 Timeline

## Evaluation Timeline





# Evaluation Process Summary



# Governing Policies

# Terminology

- ***IA Product***

- An IT product or technology whose primary purpose is to provide security services (i.e. confidentiality, authentication, integrity, access control, and non-repudiation of data); correct known vulnerabilities; and /or provide layered defense against various categories of non-authorized or malicious penetrations of information systems or networks.
- Examples: data/network encryptors, firewalls, intrusion detection systems.

# Terminology

- *IA-Enabled Product*
  - An IT product or technology whose primary role is not security, but which provides security services as an associated feature of its intended operating capabilities.
  - Examples: security-enabled web browsers, screening routers, trusted operating systems, security-enabled messaging systems

# Terminology

- *National Security System*
  - Contain classified information
  - Involves intelligence activities
  - Involves cryptographic activities related to national security
  - Involves command and control of military forces
  - Involves equipment that is an integral part of a weapon or weapons system(s)
  - Is critical to the direct fulfillment of military or intelligence missions (not including routine administrative and business applications)

# Sample IA or IA-Enabled Products

- *Operating Systems*
  - Microsoft Windows 2000 (Oct 02, EAL 4)
  - Microsoft Windows Server 2002 (In-Evaluation, EAL 4)
  - Sun Solaris 8 (Apr 03, EAL4)
- *Firewalls*
  - NetScreen Appliances Firewall (June 03, EAL 4)
  - Cryptek's DiamondTek (Jun 02, EAL 4)
- *PKI Certificate Authority*
  - RSA Keon (Dec 02, EAL 4)

# NSTISSP No. 11

- National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology Products that protect national security information.
- Effective 1 July 2002, all **COTS** IA and IA-Enabled products must be evaluated by
  - International Common Criteria Mutual Recognition Arrangement
  - NIAP Evaluation and Validation Program (CCEVS)
  - NIST FIPS validation program

# NSTISSP No 11 (cont.)

- The evaluation/validation of COTS IA and IA-enabled products will be conducted by accredited commercial laboratories, or the NIST.
- All ***GOTS*** IA or IA enabled products must be evaluated by NSA or an NSA approved process.



# Revised NSTISSP No. 11, July 2003

- Basic Policy **NOT** Changed
  - Effective 1 July 2002, all **COTS** IA and IA-Enabled products must be evaluated by:
    - International Common Criteria Mutual Recognition Arrangement
    - NIAP Evaluation and Validation Program (CCEVS)
    - NIST FIPS validation program
  - All **GOTS** IA or IA enabled products must be evaluated by NSA or an NSA approved process.

# Revised NSTISSP No. 11

- **Added Annex, Deferred Compliance Authorization (DCA) Guidelines**
  - No DCA's for encryption products.
  - DCA is for a specific COTS product for a specific application within the IT enterprise – **not** a blanket approval
  - Heads of federal departments or agencies (or their sub-delegated CIO) are the review and DCA approval authority for their respective organizations.
  - Must report DCAs to NSA/V1 for consolidated reporting to CNSS Chair.

# DoD Directive 8500.1

## 24 Oct 2002

- All IA or IA-enabled products incorporated into DoD information systems must comply with NSTISSP 11
- Products must be satisfactorily evaluated and validated either
  - prior to purchase or
  - as a condition of purchase, the vendor's products will be satisfactorily evaluated and validated.
- Purchase contracts shall specify that product validation will be maintained for subsequent releases.

# DoD Instruction 8500.2

## 12 Feb 2003

- Defines generic “robustness” levels of basic, medium, and high and assigns “baseline levels” of IA services dependent on value of information and environment
- If Government Protection Profile (PP) exist for a specific technology area
  - products must get evaluated against PP.
- If no Government PP exist for a specific technology area
  - as a condition of purchase, products must be submitted for evaluation at the appropriate EAL level as determined by ISSE and DAA.

# Public Law 107-314, 2 DEC 2002

- Passed by House Armed Services; part of Defense Authorization Bill
- Subtitle F: Information Technology, Section 352
  - Directs that Secretary of Defense is to establish a policy to limit the acquisition of information assurance technology products to those that have been evaluated and validated in accordance with appropriate criteria, schemes, or programs. Authorizes the Secretary to waive such policy for U.S. national security purposes.

# NIST Special Pub 800-23

- Applies to U.S. Civil Government
- Recommends CC evaluations/validations

# Common Criteria: Module I

## Introduction and General Model

# Scope of Common Criteria

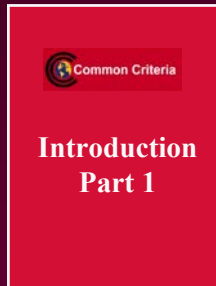
- Specification of security properties of IT systems and products that address
  - unauthorized disclosure (confidentiality, privacy)
  - unauthorized modification (integrity)
  - loss of use (availability)
- Basis for the comparison of results of independent evaluations
- Applicable to IT security countermeasures implemented in hardware, software, and firmware
  - independent of technology
  - in user-defined combinations



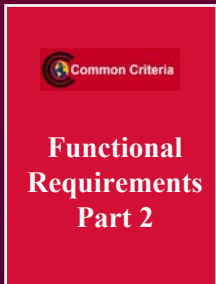
# Outside Scope of Common Criteria

- Human and physical security countermeasure implementations
- CC Application
  - ✓ administrative, legal, procedural
  - ✓ certification & accreditation processes
  - ✓ mutual recognition arrangements
- Evaluation methodology
  - ✓ Common Evaluation Methodology for Information Technology Security Evaluation (CEM)
- Cryptographic *algorithm* definition

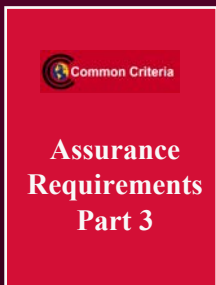
# Common Criteria Sections



- Part 1: Introduction and General Model



- Part 2: Security Functional Requirements and Annexes



- Part 3: Security Assurance Requirements

# Common Criteria Part 1

## (Introduction & General Model)

- Scope, Glossary and Overview
- Security Context and CC Approach
- Security Concepts, Environment and Objectives
- Evaluation Results
- Appendix A: History
- Appendices B: Protection Profile Specification
- Appendices C: Security Target Specification

# Common Criteria Terminology

- **Target of Evaluation (TOE)**

*An IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.*

- **Protection Profile (PP)**

*An implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs.*

- **Security Target (ST)**

*A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.*

- **TOE Security Functions (TSF)**

*A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TOE security policy (TSP).*

# Common Criteria Terminology

- **Threats**

*Any circumstance or event with the potential to cause harm to a system in the form of destruction, disclosure, modification of data, and /or denial of service.*

- **Organizational Security Policy**

*A set of rules, procedures, practices, and guidelines imposed by an organization upon its operations and to which the TOE may have to comply.*

- **Secure Usage Assumption**

*Describes the security aspects of the environment in which the TOE will be used or is intended to be used.*

- **Security Objective**

*Reflects the intent to counter identified threats and/or address any identified organizational security policies and/or assumptions.*

# General Principle

- ✓ *ALL TOE security requirements ultimately arise from consideration of the purpose and context of the TOE.*

This definition requires the PP or ST writer to define a security environment which leads to a statement of security objectives.

# Protection Profiles

- Answers the question:  
*What do I need in a security solution?*
- Implementation independent
- Multiple implementations may satisfy PP requirements
- Authors can be both consumers and producers of IT products and systems

# Security Targets

- Answers the question:  
*What do you provide in a security solution?*
- Implementation dependent/specific
- Authors can be product vendors, product developers, or product integrators



# Protection Profiles and Security Targets

- PP makes a statement of implementation independent security needs
  - *a generic operating system with discretionary access controls, audit, and identification and authentication*
- ST defines the implementation dependent capabilities of a *specific* product, e.g.
  - *Microsoft NT 4.0.0.2 (TOE)*
  - *Sun OS 4.7.4 (TOE)*

# PP/ST Comparison

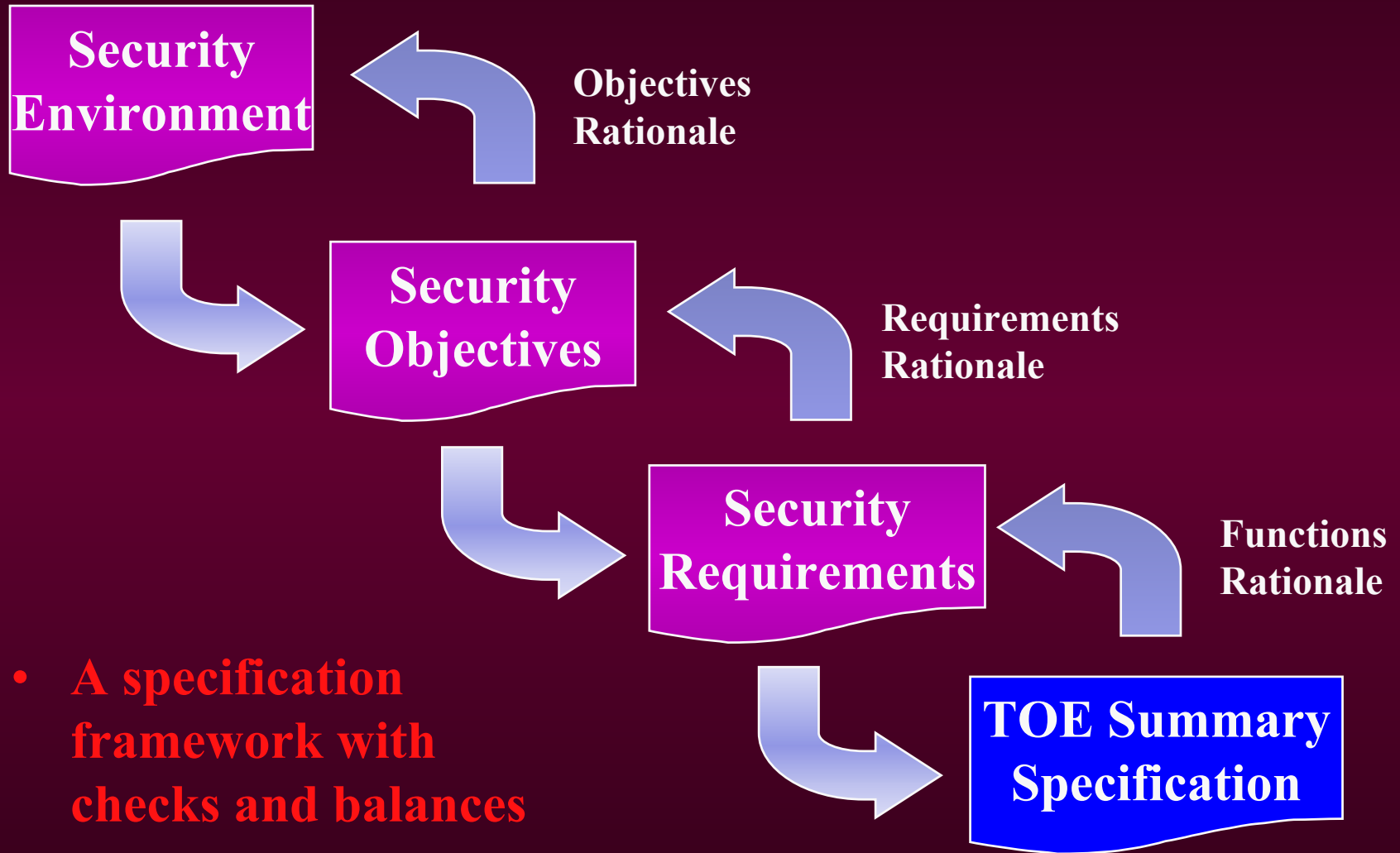
## *Protection Profile*

- Identification
- Overview
- TOE Description
- Security Environment
- Security Objectives
- Security Requirements
- Rationale

## *Security Target*

- Identification
- Overview
- TOE Description
- Security Environment
- Security Objectives
- Security Requirements
- Rationale
- TOE Summary Specification
- CC Conformance Claim
- PP Claims

# PP/ST Specification Framework



# Establishing a Security Environment

## Things to Consider---

- ✓ TOE physical environment
- ✓ Assets/Resources requiring protection
- ✓ TOE purpose

# TOE Security Environment

- Secure Usage Assumptions
  - ✓ *The non-IT security aspects of the environment in which the TOE will be used or is intended to be used.*
- Threats
  - ✓ *The ability to exploit a vulnerability by a threat agent.*
- Organizational Security Policies
  - ✓ *A set of rules, procedures, practices, or guidelines imposed by an organization upon its operations.*

# Secure Usage Assumptions

- Describes the security aspects of the environment in which the TOE will be used or is intended to be used
- Information about intended usage and the environment---
  - ✓ intended application, potential asset value, and usage limitations
  - ✓ physical issues, connectivity issues, and personnel issues
  - ✓ must not impose requirements on the TOE or on its IT environment
  - ✓ generate objectives for the (non-IT) environment

# Threat

- The ability of a *threat agent* to mount *an attack* on an *asset*, and the *result* of that attack
- Threats provide a basis for statement of countermeasures
- A well-written threat statement addresses
  - ✓ Threat Agent and/or Attacker
  - ✓ The Attack
  - ✓ Assets
  - ✓ Results



# Security Policies

- Organizational Security Policy:  
*A set of rules, procedures, practices, and guidelines imposed by an organization upon its operations and to which the TOE may have to comply.*
- Organizationally-Imposed Requirements
  - *Passwords Shall Be 8 Characters*
  - *Cryptography Shall Be Used for Intra-Node Communication*



# Environment Examples

- **A.Physical\_Protection**

*The TOE is installed in a restricted and controlled access area sufficient to prevent unauthorized physical access to the TOE.*

- **T.Intercept**

*An non-administrative user obtains unauthorized access to controlled information by intercepting information transmitted to/from the TOE.*

- **P.Accountability**

*The authorized users of the TOE shall be held accountable for their actions within the TOE.*

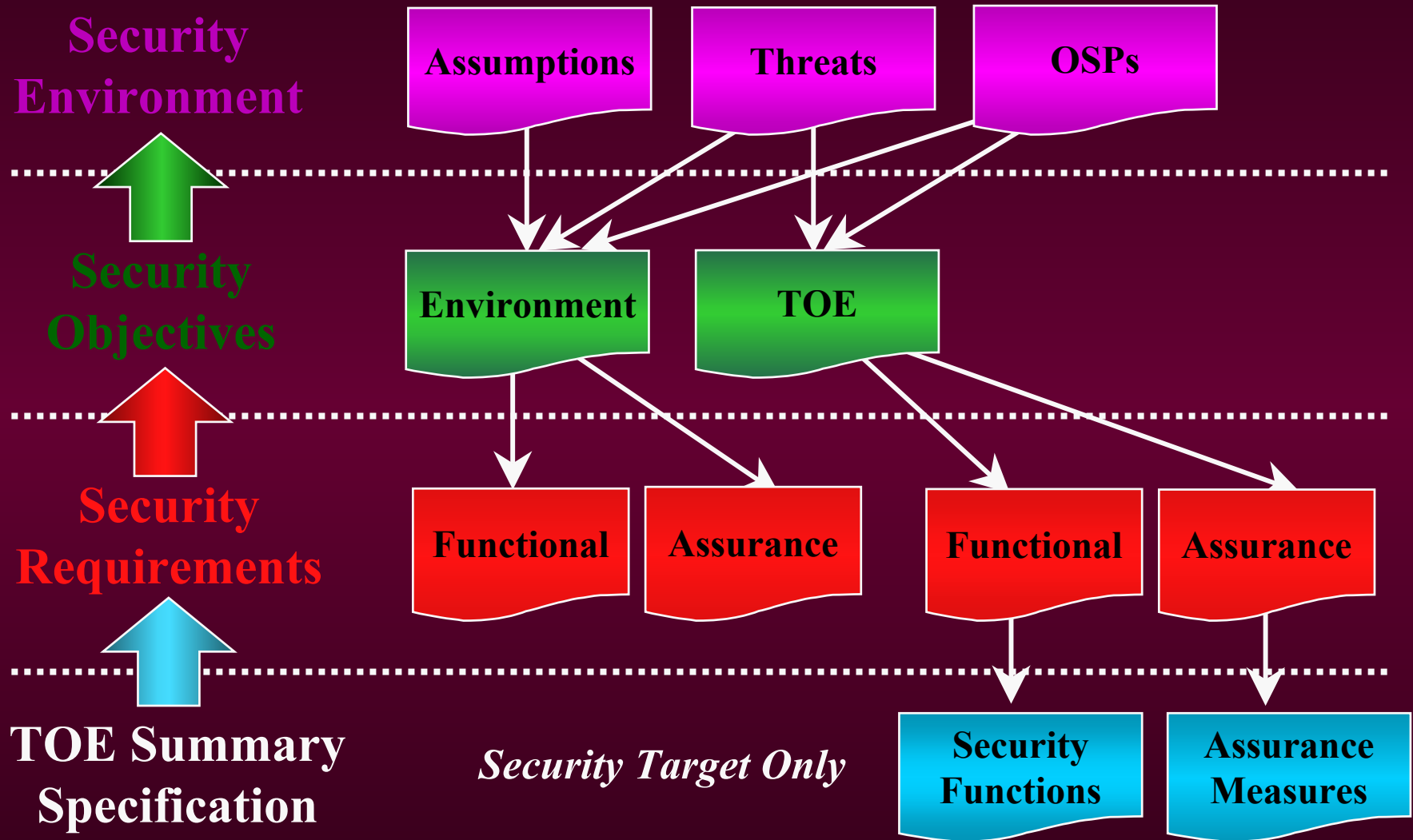
# Security Objectives

- Establish the basis for the selection of security requirements (functional & assurance)
- Based completely upon the statement of the security environment
- Objectives describe
  - ✓ Support for assumptions
  - ✓ Mitigation of threats (eliminate, minimize, monitor)
  - ✓ Enforcement organizational security policy

# Types of Security Objectives

- Security objectives for the TOE
  - ✓ *Implemented by security requirements allocated to the TOE*
- Security objectives for the environment
  - ✓ *Implemented by security requirements allocated to the IT systems that interact with the TOE*
  - ✓ *Implemented by personnel and procedural means*
  - ✓ *Outside the scope of the CC*

# PP/ST Framework



# Crafting PPs / STs

- “Top Down” approach
  - Usually PPs
  - Start with environment
  - Derive Objectives
  - Select Requirements
- “Technology Specific” approach
  - Usually PPs
  - Survey products in technology (requirements)
  - Identify function in environment
  - Complete specification
- “Product” approach
  - Usually STs
  - Define what product does (functional requirements)
  - Define existing documentation/assurance (assurance requirements)
  - “Back in” environment

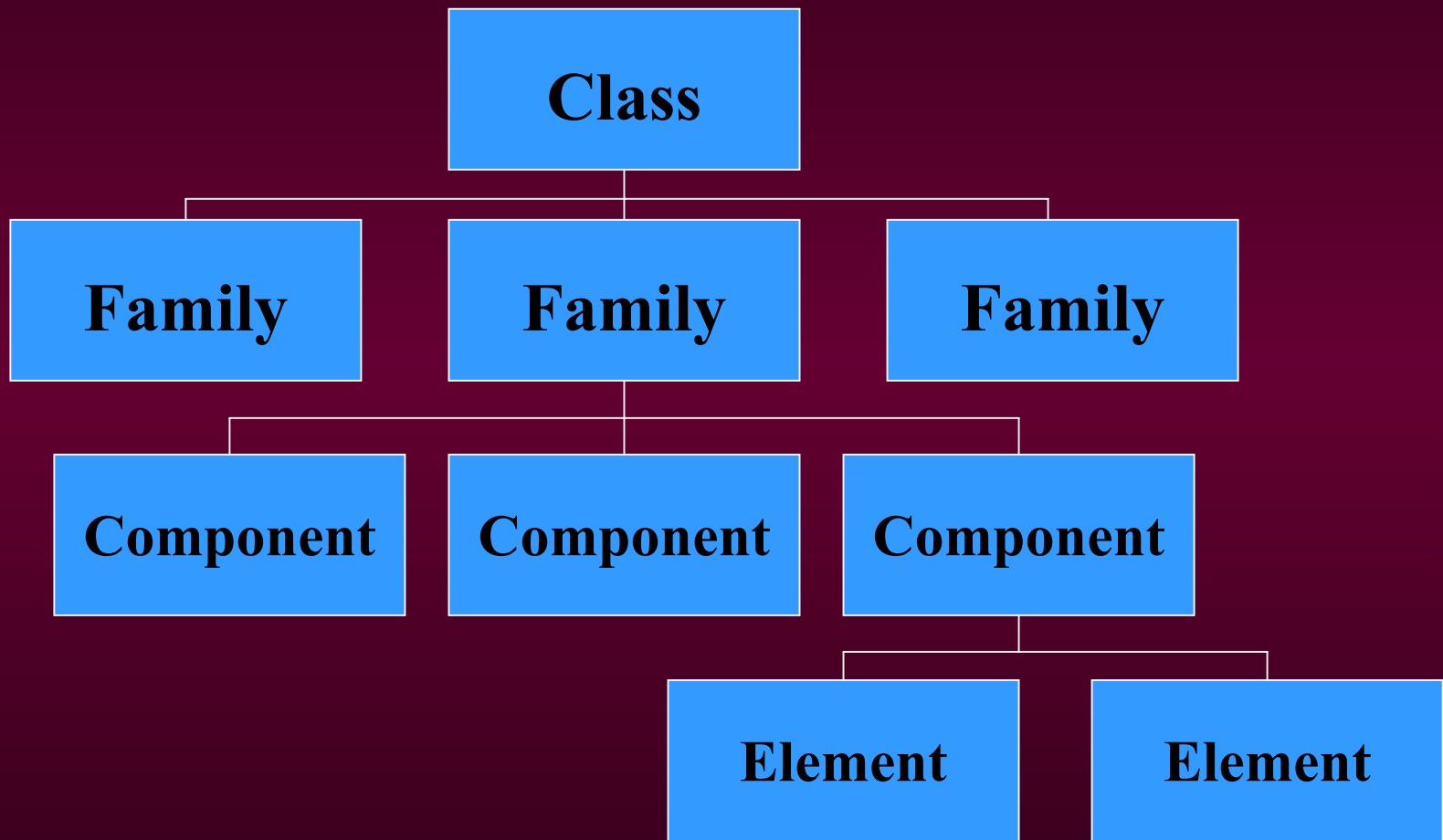
# Module II

## Security Functional Requirements

# Security Functional Requirements

*Levied upon functions of the TOE that support IT security; their behavior can generally be observed.*

# Hierarchy of Requirements (Functional)





# Definitions

- **Class** - for organizational purposes; all members share a common intent but differ in coverage of security objectives.
- **Family** - for organizational purposes; all members share security objectives but differ in rigor or emphasis
- **Component** - describes an actual set of security requirements; smallest selectable set
- **Element** - members of a component; cannot be selected individually; explicit shall statements

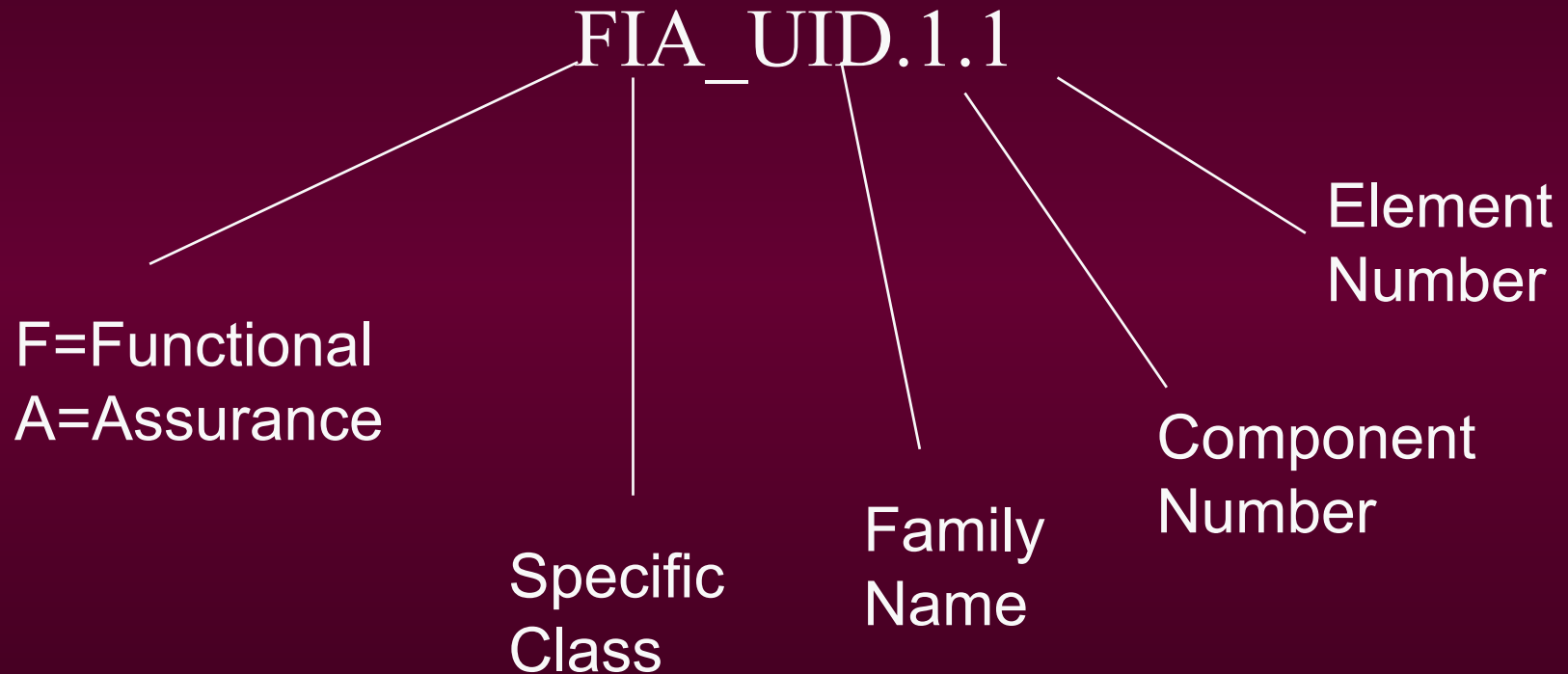
# Security Functional Classes

- ✓ Security Audit (FAU)
- ✓ Communications (FCO)
- ✓ Cryptographic Support (FCS)
- ✓ User Data Protection (FDP)
- ✓ Identification & Authentication (FIA)
- ✓ Security Management (FMT)

# Security Functional Classes

- ✓ Privacy (FPR)
- ✓ Protection of the Trusted Security Functions (FPT)
- ✓ Resource Utilization (FRU)
- ✓ TOE Access (FTA)
- ✓ Trusted Path (FTP)

# Interpreting Functional Requirement Names



# Functional Family Structure

## FIA\_UID User Identification

### Family behavior

This family defines the conditions under which users shall be required to identify themselves before performing any other actions that are to be mediated by the TSF and which require user identification.

### Component leveling



FIA\_UID.1 Timing of identification, allows users to perform certain actions before being identified by the TSF.

FIA\_UID.2 User identification before any action, require that users identify themselves before any action will be allowed by the TSF.

# Functional Family Structure

## **Management: FIA\_UID.1**

The following actions should be considered for the management functions in FMT:

- a) the management of the user identities;
- b) if an authorized administrator can change the actions allowed before identification, the managing of the action lists.

## **Management: FIA\_UID.2**

The following actions should be considered for the management functions in FMT:

- a) the management of the user identities.

## **Audit: FIA\_UID.1, FIA\_UID.2**

The following actions should be auditable if FAU\_GEN Security Audit Data Generation is included in the PP/ST:

- a) Minimal: Unsuccessful use of the user identification mechanism, including the user identity provided.
- b) Basic: All use of the user identification mechanism, including the user identity provided.

# Functional Family Structure

## FIA\_UID.1

### Timing of Identification

Hierarchical to: no other components.

#### FIA\_UID.1.1

The TSF shall allow [assignment: *[list of TSF-mediated actions]*] on behalf of the user to be performed before the user is identified.

#### FIA\_UID.1.2

The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: **No dependencies**

# Functional Family Structure

**FIA\_UID.2**

**User Identification before any action**

Hierarchical to: FIA.UID.1

**FIA\_UID.2.1**

**The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.**

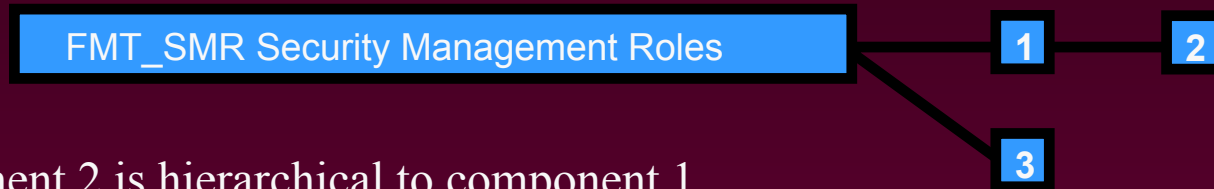
Dependencies: **No dependencies**



# Component Hierarchy

- Each family contains one or more components
- The component leveling diagram depicts the relationship between components in a family
  - no relationship, or
  - a hierarchical relationship
- A hierarchical component
  - satisfies any dependency on the component it is hierarchical to
  - may provide more security or more functionality than a component it is hierarchical to
- Hierarchical components are not selected together within the same context of the PP/ST

# Component Hierarchy Examples



Component 2 is hierarchical to component 1

Component 3 is not hierarchically related to either component 1 or 2

Legal component selections are: Component 1, Component 2, Component 3, Components 1 and 3, Components 2 and 3



Component 2 is hierarchical to component 1

Component 3 is hierarchical to component 1

Component 4 is hierarchical to component 3

Legal component selections are: Component 1, Component 2, Component 3, Component 4, Components 2 and 3, Components 2 and 4

# Class FAU: Security Audit

- Common Intent: The six families in this class are concerned with ...
    - recognizing and responding to (FAU\_SAA, FAU\_ARP)
    - recording (FAU\_GEN, FAU\_SEL)
    - storing and protecting (FAU\_STG)
    - review and analysis of (FAU\_SAR)
- ... security-relevant events and activities.

# Class FAU: Security Audit

## (An Example)

### NEED:

A record of certain actions taken by users such that an administrator can determine when the action occurred, who did it, whether it succeeded or failed.

### TO SATISFY:

- ✓ FAU\_GEN.1 Audit Data Generation
- ✓ FAU\_GEN.2 User Identity Association

# Class FCO: Communication

- Common Intent: The two families in this class are concerned with ...
  - proof of origin (FCO\_NRO)
  - proof of receipt (FCO\_NRR)

... of transmitted information.

# Class FCO: Communication

## (An Example)

### NEED:

The recipient of all email messages must be able to verify the identity of the sender.

### TO SATISFY:

- ✓ FCO\_NRO.1 Selective Proof of Origin
- ✓ FCO\_NRO.2 Enforced Proof of Origin (more functionality)

# Class FCS: Cryptographic Support

- Common Intent: The two families in this class are concerned with ...
  - Generation, distribution, access, and destruction (FCS\_CKM)
  - operational use (FCS\_COP)

... of cryptographic keys.

# Class FCS: Cryptographic Support (An Example)

## NEED:

An administrator must generate and distribute cryptographic keys according to the appropriate algorithms and distribution, respectively.

## TO SATISFY:

- ✓ FCS\_CKM.1 Cryptographic Key Generation
- ✓ FCS\_CKM.2 Cryptographic Key Distribution



# Class FDP: User Data Protection

- Common Intent: The thirteen families in this class are concerned with ...
  - security function policies (FDP\_ACC, FDP\_IFC)
  - forms of user data protection (FDP\_ACF, FDP\_IFF, FDP\_ITT, FDP\_RIP, FDP\_ROL, FDP\_SDI)
  - import/export (FDP\_DAU, FDP\_ETC, FDP\_ITC)
  - inter-TSF communications (FDP\_UCT, FDP\_UIT)

... for data protection.

# Class FDP: User Data Protection

## (An Example)

### NEED:

When a user data file is deleted its contents must be inaccessible and when a new one is created it should contain no previous information.

### TO SATISFY:

- ✓ FDP\_RIP.2 Full Residual Information Protection

# Class FIA: Identification & Authentication

- Common Intent: The six families in this class are concerned with ...
  - identification (FIA\_UID)
  - authentication (FIA\_UAU, FIA\_SOS, FIA\_AFL)
  - attributes (FIA\_ATD, FIA\_USB)

... of a user.

# Class FIA: Identification & Authentication

## (An Example)

### NEED:

An individual may only attempt to log into the system 3 times. After that, if the attempts are not successful, the individual's account shall be locked until unlocked by an administrator.

### TO SATISFY:

- ✓ FIA\_AFL.1 Basic Authentication Handling

# Class FMT: Security Management

- Common Intent: The six families in this class are concerned with ...
  - management of TSF data (FMT\_MTD)
  - management of security attributes (FMT\_MSA, FMT\_REV, FMT\_SAE)
  - management of security functions (FMT\_MOF)
  - security roles (FMT\_SMR)

... of the TOE.

# Class FMT: Security Management

## (An Example)

### NEED:

Our organization has a security officer responsible for new users and I&A functions; and an audit administrator responsible for the audit mechanism.

### TO SATISFY:

- ✓ FMT\_SMR.1 Security Management Roles
- ✓ FMT\_MTD.1 Management of TSF Data

# Class FPR: Privacy

- Common Intent: The four families in this class are concerned with protection against ...
  - discovery and misuse (FPR\_ANO, FPR\_PSE, FPR\_UNL, FPR\_UNO)

... of an individual's identity by others.

# Class FPR: Privacy

## (An Example)

### NEED:

A web page's content and questionnaire deal with a sensitive public health issue. It is important that respondents be assured of complete unobservability when reading the data and filling out of the form. There is also no reason for even an administrator to be capable of identifying individuals who choose to respond. Without such assurance, people will be reluctant to respond and the sponsoring authority will not get accurate data.

### TO SATISFY:

- ✓ FPR\_UNO.1 Unobservability



# Class FPT: Protection of the Trusted Security Functions

- The sixteen families in this class address ...
  - reference mediation and domain separation (FPT\_RVM, FPT\_SEP)
  - testing (FPT\_AMT, FPT\_TSF)
  - physical/anti-tamper protection (FPT\_PHP)
  - secure TSF data transfer (FPT\_ITA, FPT\_ITC, FPT\_ITI, FPT\_ITT, FPT\_RPL, FPT\_TDC, FPT\_TRC)
  - failure and recovery (FPT\_RCV, FPT\_FLS)
  - state and timing (FPT\_SSP, FPT\_STM)

... of the TSF mechanisms and data.

# Class FPT: Protection of the Trusted Security Functions (An Example)

## NEED:

An authorized administrator must be able to verify that the executables that implement the security functions have not been modified by malicious individuals or code.

## TO SATISFY:

- ✓ FPT\_TST.1 TSF Self Test

# Class FRU: Resource Utilization

- Common Intent: The three families in this class are concerned with ...
  - availability (FRU\_FLT)
  - allocation (FRU\_PRS, FRU\_RSA)

... of resources.

# Class FRU: Resource Utilization

## (An Example)

### NEED:

A denial of service attack by a user consuming all available disk space must be prevented.

### TO SATISFY:

- ✓ FRU\_RSA.1 Maximum Quotas

# Class FTA: TOE Access

- Common Intent: The six families in this class are concerned with ...
    - attributes (FTA\_LSA, FTA\_TAB, FTA\_TAH)
    - establishment and control (FTA\_MCS, FTA\_SSL, FTA\_TSE)
- ... of a user session.

# Class FTA: TOE Access

## (An Example)

### NEED:

Whenever a user session remains idle for a specified period of time, the session shall be automatically locked by the system. Also, individuals shall have the ability to lock their own sessions.

### TO SATISFY:

- ✓ FTA\_SSL.1 TSF-Initiated Locking
- ✓ FTA\_SSL.2 User-Initiated Locking

# Class FTP: Trusted Path/Channels

- Common Intent: The two families in this class are concerned with ...
  - trusted communication paths (FTP\_TRP)
  - trusted communication channels (FTP\_ITC)
- ... between users and the TSF; and between the TSF and other trusted IT products, respectively.

# Class FTP: Trusted Path/Channel

## (An Example)

### NEED:

There must be a means by which remote administrators can verify that they are communicating with the TSF.

### TO SATISFY:

- ✓ FTP\_TRP.1 Trusted Path



# Requirements Rationale

- Threats/OSPs (through security objectives) drive functional requirement selection
- Rationale must demonstrate that the functional requirements are *suitable to meet and traceable to* the security objectives
- The rationale must demonstrate:
  - ✓ why the choice of security requirements meets an objective
  - ✓ functional & assurance requirements are not contradictory and are complete
  - ✓ strength of function (SOF) claims are consistent with the security objectives

# Operations on Requirements

## (Functional)

- Types of operations
  - ✓ assignment
  - ✓ selection
  - ✓ refinement
  - ✓ iteration
- Functional requirements have placeholders indicating where assignment and selection operations are allowed
- Refinement and iteration may be performed on any functional requirement

# Assignment Operations

- Specification of a parameter filled in when component is used
- “Fill in the Blank” operation
- Allows PP/ST writer to provide information relating to application of the requirement
- The PP writer may defer completing assignments, but the ST writer must complete all assignments

# Assignment Operation

## (An Example)

*As Written in the Common Criteria:*

- **FMT\_SMR.1.1** The TSF shall maintain the roles:  
[assignment: *the authorized identified roles*].

*After Assignment Operation:*

- **FMT\_SMR.1.1** The TSF shall maintain the roles:  
[*auditor, security administrator, operator*].

# Selection Operations

- Specification of elements selected from a list given in the component
- “Multiple Choice” operation
- Allows PP/ST writer to select from a provided list of choices
- The PP writer may defer completing selections, but the ST writer must complete all selections

# Selection Operation

## (An Example)

*As Written in the Common Criteria:*

- **FTA\_TAH.1.1** Upon successful session establishment, the TSF shall display the [selection: *date, time, method, location*] of the last successful session establishment to the user.

*After Selection Operation:*

- **FTA\_TAH.1.1** Upon successful session establishment, the TSF shall display the [*date, time, and location*] of the last successful session establishment to the user

# Selection and Assignment

## (An Example)

*As Written in the Common Criteria:*

- **FMT\_MTD.1.1** The TSF shall restrict the ability to [selection: *change\_default, query, modify, delete, clear*, [assignment: *other operations*]] the [assignment: *list of TSF data*] to [assignment: *the authorised identified roles*].

*After Operations:*

- **FMT\_MTD.1.1** The TSF shall restrict the ability to [*delete*, [and create]] the [user authentication database] to [*the security administrator*].

# Refinement Operations

- A mechanism to tailor a requirement by specifying additional detail in order to meet a security objective
- Can be performed on any functional component
- Rules for refinement:
  - ✓ the refinement shall only restrict the set of possible acceptable functions used to implement the requirement
  - ✓ the refinement may not levy completely new requirements
  - ✓ the refinement may not increase the list of dependencies of the requirement being refined
  - ✓ the refinement may provide an elaboration or interpretation
  - ✓ the refinement may not eliminate the requirement



# Refinement Operation

## (An Example)

*As Written in the Common Criteria:*

- **FAU\_SAA.1.1** The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the TSP.

*After Refinement Operation:*

- **FAU\_SAA.1.1** The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the TSP *by notifying the Security Officer immediately.*

# Iteration Operations

- Repetitive use of the same component to address different aspects of the requirement being stated (e.g., identification of more than one type of user).
- Can be performed on any functional component

# Iteration Operation

## (An Example)

*As Written in the Common Criteria:*

- **FMT\_MTD.1.1** The TSF shall restrict the ability to [selection: *change\_default, query, modify, delete, clear*, [assignment: *other operations*]] the [assignment: *list of TSF data*] to [assignment: *the authorized identified roles*].

*After Iteration Operation:*

- **FMT\_MTD.1.1(1)** The TSF shall restrict the ability to [*modify*] the [*enrolled images db*] to [*the security administrator*].
- **FMT\_MTD.1.1(2)** The TSF shall restrict the ability to [*backup/restore*] the [*enrolled images db*] to [*the operator*].

# Dependencies

## (Functional Components)

- Some requirement components are not self sufficient
- Some functional requirement components have functional and assurance dependencies
- Some dependencies may be eliminated with sufficient rationale

# Common Criteria Part 2: Annexes

- Annex A:  
*Security Functional Requirements Application Notes*
  - Dependency Table
- Annexes B - M:  
*Similar to Part 2 but more informative*
  - ✓ user notes
  - ✓ evaluator notes
  - ✓ documentation notes

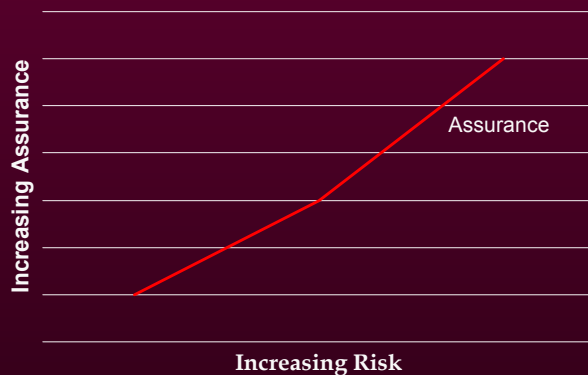
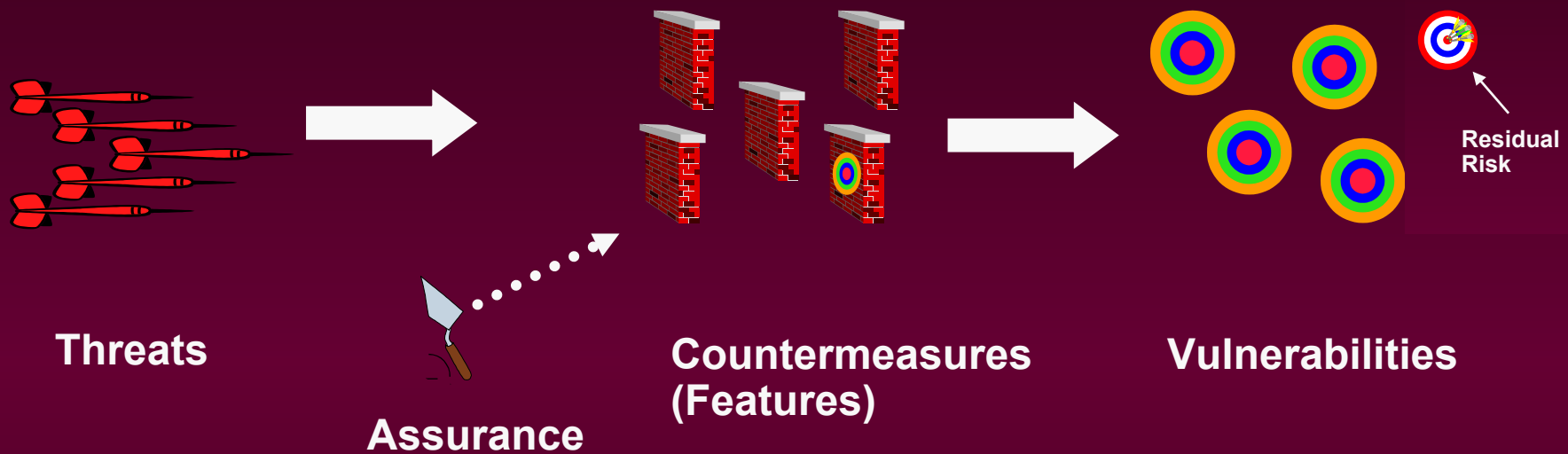
# Module III

## Security Assurance Requirements

# What is Assurance?


*Assurance is a property of the TOE which gives confidence that the claimed security measures of the TOE are effective and implemented correctly.*

# Why Do We Care About Assurance?





# How Do We Gain Assurance?

- Analysis of the correspondence between TOE design representations
  - Analysis of the TOE design representations against the requirements
- 
- Analysis of functional tests coverage, and results
  - Independent functional testing
  - Penetration testing
- Verification of mathematical proofs
  - Analysis of guidance documents
  - Analysis of processes and procedures
  - Checking that processes and procedures are being applied

# Evaluation Assurance Scale

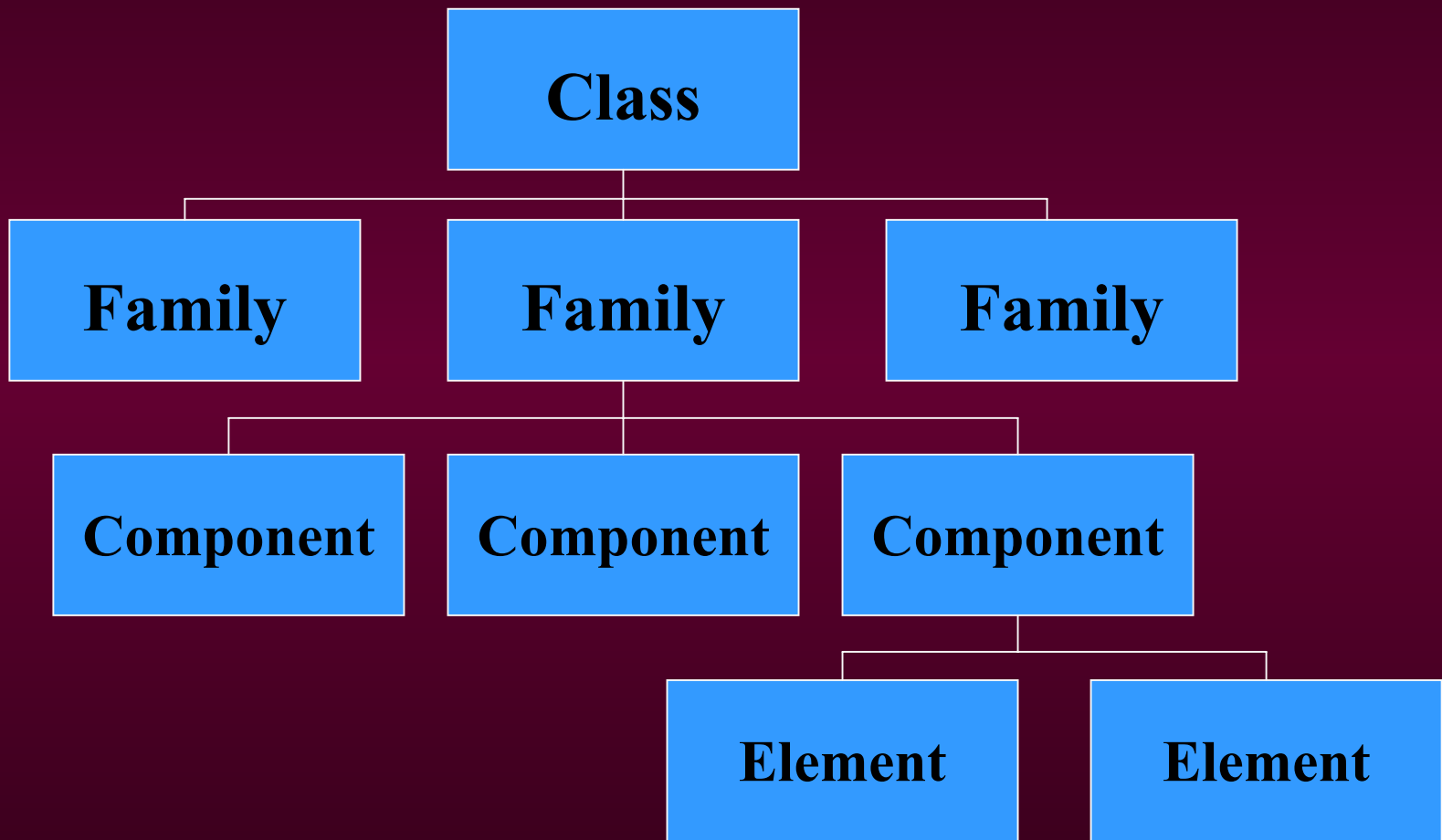
Greater Evaluation Effort  
(Scope, Depth, Rigor)



Greater  
Assurance

# Hierarchy of Requirements

(Assurance)



# Definitions

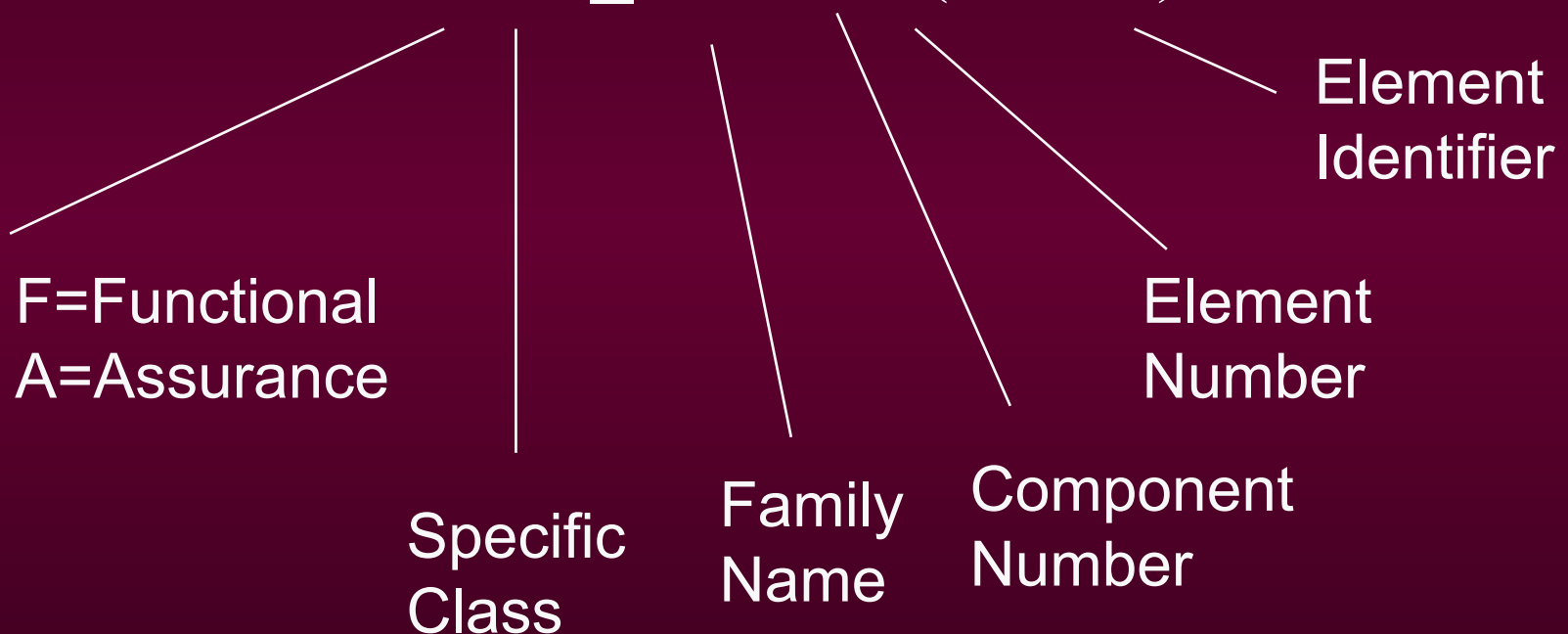
- **Class** - for organizational purposes; all members share a common intent but differ in coverage of security objectives.
- **Family** - for organizational purposes; all members share security objectives but differ in rigor or emphasis
- **Component** - describes an actual set of security requirements; smallest selectable set
- **Element** - members of a component; cannot be selected individually; explicit shall statements

# Security Assurance Classes

- ✓ Configuration Management (ACM)
- ✓ Delivery and operation (ADO)
- ✓ Development (ADV)
- ✓ Guidance documents (AGD)
- ✓ Life Cycle Support (ALC)
- ✓ Tests (ATE)
- ✓ Vulnerability assessment (AVA)
- ✓ Evaluation Criteria (APE, ASE)
- ✓ Assurance Maintenance (AMA)

# Interpreting Assurance Requirement Names

ADV\_LLD.3.1(D,C,E)



# Class ACM: Configuration Management

- Common Intent: The three families in this class are concerned with ...
  - protecting the integrity (ACM\_SCP)
  - tracking/restricting the modification (ACM\_AUT, ACM\_CAP)

... of configuration items.

# Class ADO: Delivery and Operation

- Common Intent: The two families in this class are concerned with ...
  - delivery (ADO\_DEL)
  - installation, generation, start-up (ADO\_IGS)

... of the TOE.

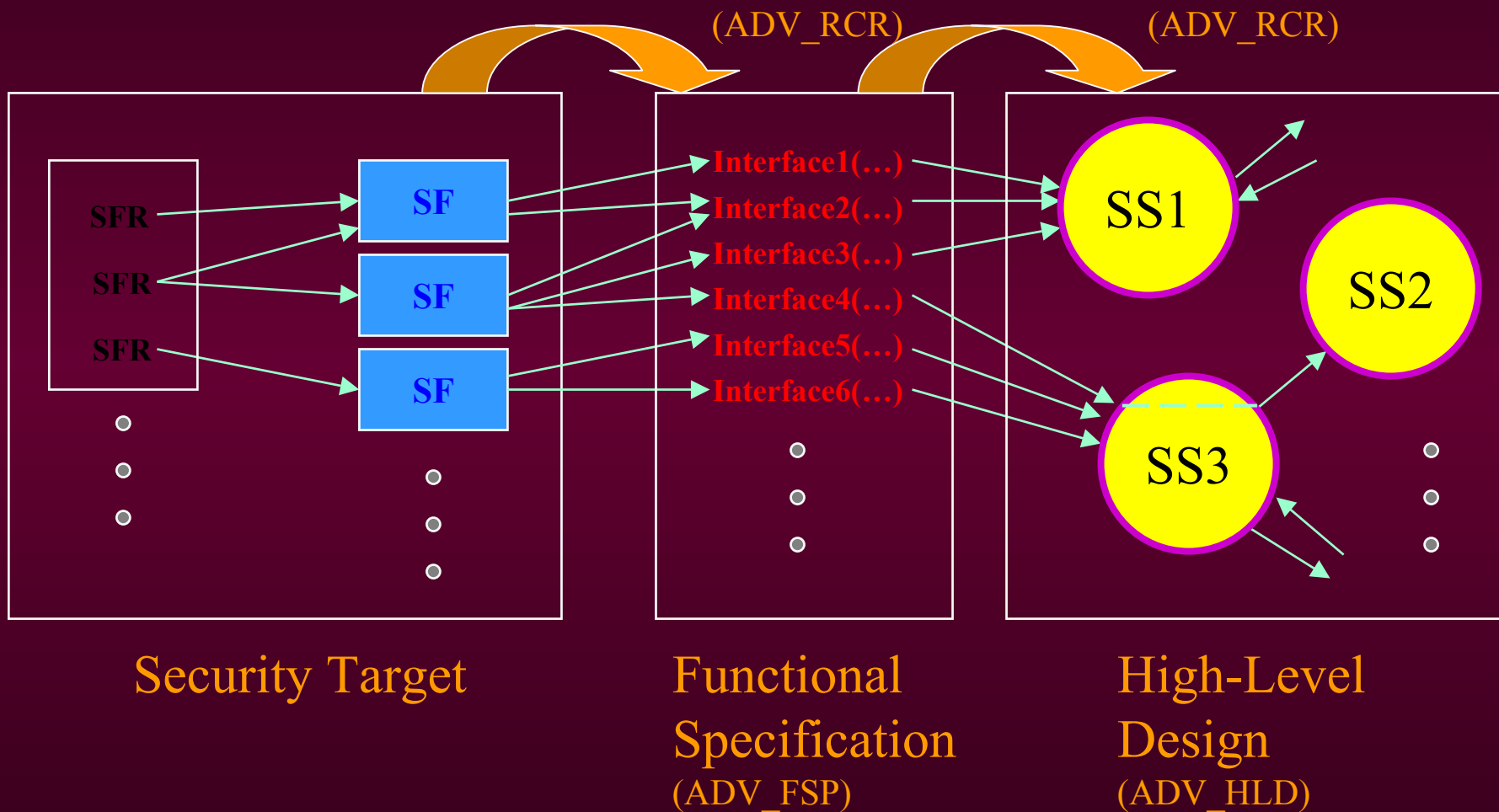


# Class ADV: Development

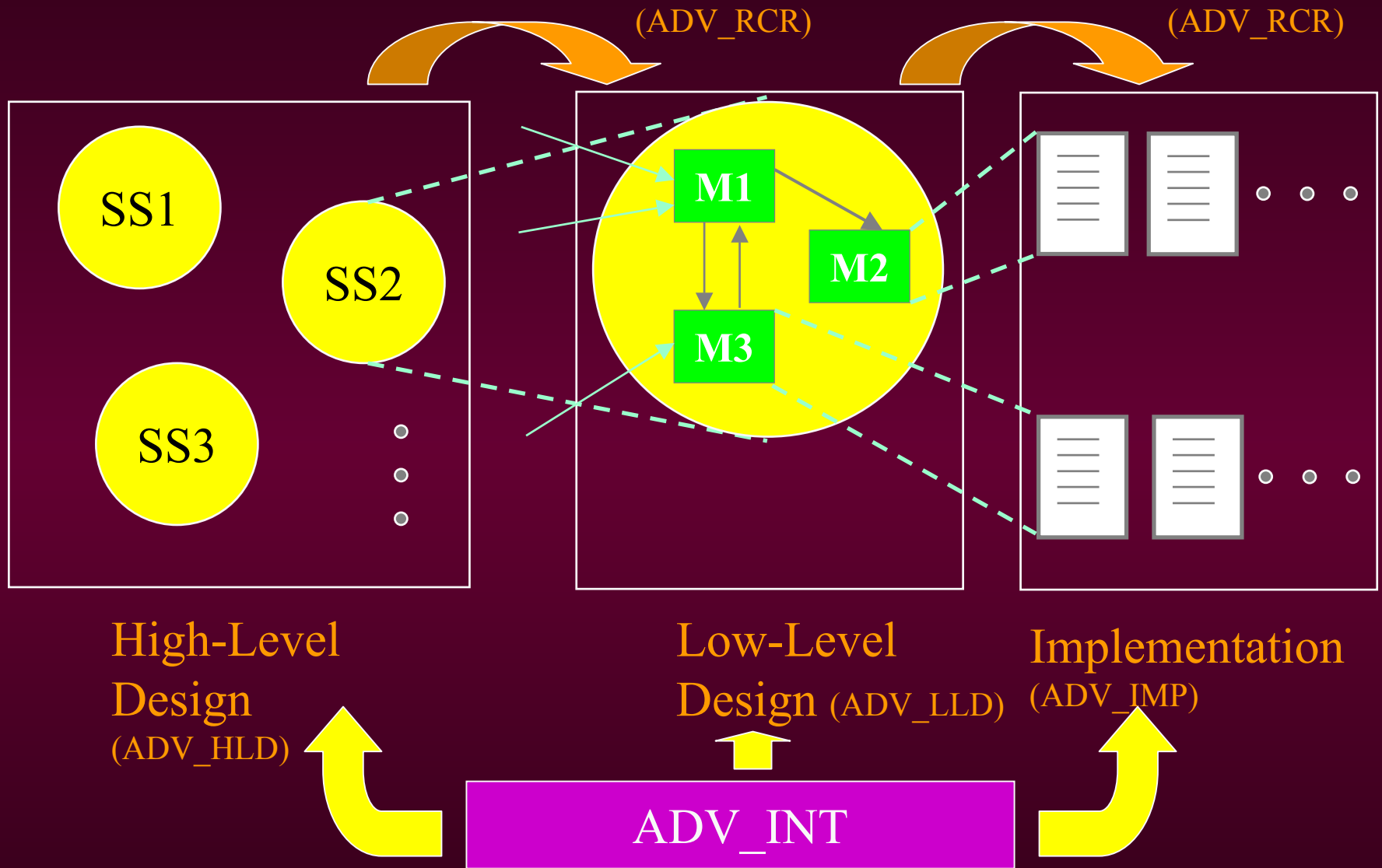
- Common Intent: The seven families in this class are concerned with ...
  - levels of abstraction (ADV\_FSP, ADV\_HLD, ADV\_IMP, ADV\_LLD)
  - correspondence mapping of representations (ADV\_RCR)
  - internal structure (ADV\_INT)
  - policy model (ADV\_SPM)

... of the TSF.

# ADV Overview



# ADV Overview



# Class AGD: Guidance Documents

- Common Intent: The two families in this class are concerned with ...
    - user (AGD\_USR)
    - administrator (AGD\_ADM)
- ... guidance documentation.

# Class ALC: Life Cycle Support

- Common Intent: The four families in this class are concerned with refinement of the TOE during ...
  - development (ALC\_DVS, ALC\_FLR)
  - maintenance (ALC\_LCD, ALC\_TAT)

... phases.

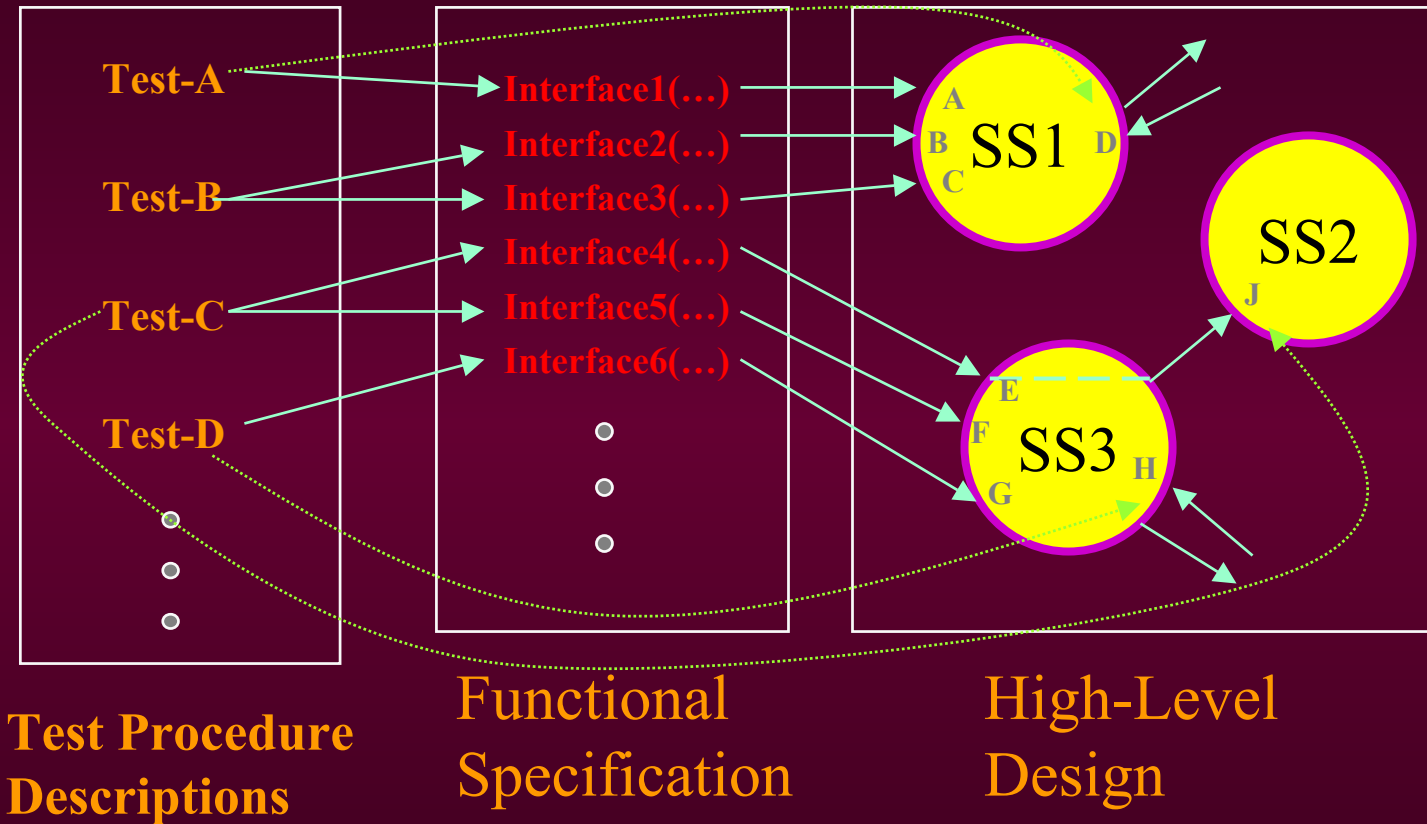
# Class AMA: Maintenance of Assurance

- Common Intent: The four families in this class are concerned with...
    - maintenance planning & procedures (AMA\_AMP, AMA\_EVD)
    - maintenance activities (AMA\_CAT, AMA\_SIA)
- ... after a TOE has been evaluated against the CC.

# Class ATE: Tests

- Common Intent: The four families in this class are concerned with ...
    - coverage (ATE\_COV)
    - depth (ATE\_DPT)
    - vendor functional and independent (ATE\_FUN)
    - evaluator independent (ATE\_IND)
- ... testing.

# ATE\_COV, ATE\_DPT





# Class AVA: Vulnerability Assessment

- Common Intent: The four families in this class are concerned with ...
  - exploitable covert channels (AVA\_CCA)
  - misuse (AVA\_MSU)
  - vulnerabilities and strength (AVA\_VLA, AVA\_SOF)

... of the TOE.

# Class APE: Protection Profile Evaluation

- Common Intent: The six families in this class are concerned with ...
    - complete, consistent, and technically sound (APE\_DES, APE\_ENV, APE\_INT, APE\_OBJ, APE\_REQ, APE\_SRE)
- ... protection profiles.

# Class ASE: Security Target Evaluation

- Common Intent: The eight families in this class are concerned with ...
    - complete, consistent, and technically sound (ASE\_DES, ASE\_ENV, ASE\_INT, ASE\_OBJ, ASE\_PPC, ASE\_REQ, ASE\_SRE, ASE\_TSS)
- ... security targets that are suitable for TOE specification.

# Dependencies

## (Assurance Components)

- Dependencies have same meaning as for functional requirements
- Table A.1 (Part 2: Annexes page 4) identifies all dependencies
  - direct (as stated in the requirement)
  - indirect (as a result of “chasing down” the dependencies)

# Operations on Requirements

## (Assurance)

- Iteration
- Refinement

# Requirements Packages

- Reusable set of *functional* or *assurance* components combined together to satisfy a set of identified security objectives
- In CC Part 3 there are 7 assurance packages called Evaluation Assurance Levels (increasing rigor and formalism from EAL1 to EAL7)
- Packages being specified for levels of robustness
  - Basic and Medium are in draft
  - High is still being defined

# Evaluation Assurance Levels (EALs)

- Provide an increasing scale
- This scale balances:
  - ✓ level of assurance obtained
  - ✓ cost/feasibility of acquiring it

# Considerations for EAL Selection

- ✓ Value of the assets
- ✓ Risk of the assets being compromised
- ✓ Current state of practice in definition and construction of the TOE
- ✓ Security Environment
- ✓ Development, evaluation, & maintenance costs
- ✓ Resources of adversaries
- ✓ Functional requirement dependencies



# EAL1 - Functionally Tested

- Confidence in current operation is required
- No assistance from TOE developer
- Applicable where threat to security is not serious
- Incomplete independent testing against specification and guidance documentation

# EAL2: Structurally Tested

- Requires some cooperation of the developer
- Low to moderate of independently assured security
- Adds requirements for configuration list, delivery, high-level design documentation, developer functional testing, vulnerability analysis, more extensive (but still not complete) independent testing

# EAL3: Methodically Tested and Checked

- Requires positive security engineering at the design stage without substantial changes in existing practices
- Moderate assurance through investigation of product and development environment controls, and high-level design documentation
- Places additional requirements on testing (now complete), development environment controls and TOE configuration management

# EAL4: Methodically Designed, Tested, and Reviewed

- Requires security engineering based on good commercial development practices
- Highest level likely for retrofit of an existing product
- Additional requirements on design, implementation, vulnerability analysis, low level design documentation, development and system automated configuration management, and an informal security policy model

# EAL5: Semiformally Designed and Tested

- Higher assurance, risk situations
- Requires rigorous commercial development practices and moderate use of specialist engineering techniques
- Introduces structured implementation of TSF
- Additional requirements on semi-formal functional specification, high-level design, and their correspondence, increased vulnerability testing, full implementation representation, and covert channel analysis

# EAL6: Semiformally Verified Design and Tested

- Applicable to a rigorous development environment
- High assurance for high value assets/risk situations
- Additional requirements on analysis, layered TOE design, semi-formal low-level design documentation, complete CM system automation and a structured development environment, and increased vulnerability testing/covert channel analysis

# EAL7: Formally Verified Design and Tested

- Maximum assurance for extremely high risk situations
- Generally for experimental application
- Assurance is gained through application of formal methods in the documentation of the functional specification and high-level design
- Additional requirements for complete developer test analysis, complete independent confirmation of the test results, and complete documentation of the structure of the TSF

# EAL Augmentation

- The tailoring of an existing Evaluation Assurance Level (EAL)
  - ✓ Specify assurance component(s) in addition to those in an existing EAL
- Allowed augmentation operations
  - ✓ Specify a higher component in the same family
  - ✓ Specify a higher component from another family
  - ✓ Specify new components that are not contained in an EAL
- Disallowed augmentation operation
  - ✓ Removal of components from an EAL definition



# U.S. Government Packages

- Based on DoDI 8500.2 and NIST guidance, U.S. Government Protection Profiles are developed according to the following defined packages:
  - U.S. Government Basic Robustness
  - U.S. Government Medium Robustness
  - U.S. Government High Robustness

# Basic Robustness

- Basic Robustness provides assurance by an analysis of the TOE security functions using
  - guidance documentation,
  - functional specification,
  - high level design, and
  - interface specification.
- EAL 2 augmented portions require
  - accuracy of system documentation,
  - the tracking and correction of system flaws.

# Basic Robustness (cont.)

- Assurance requirements include all components of EAL 2 augmented with
  - ✓ Flaw Reporting Procedures (ALC\_FLR.2)
  - ✓ Examination of Guidance (AVA\_MSU.1)
- Allow “Partial” TOEs
  - ✓ Software only
  - ✓ Portion of system (e.g., database only)

# Medium Robustness

- Medium robustness provides assurance by an analysis of the TOE security functions using
  - architectural design documents,
  - low-level design of the TOE,
  - implementation representation of the entire TSF,
  - complete interface specifications,
  - systematic cryptographic module covert channel,
  - informal TOE security policy model, and
  - modular TOE design.
- Allow only “complete” TOEs (i.e. hardware, operating system, and application software are required).

# Medium Robustness (cont)

- Medium robustness includes components of EAL 4 augmented with
  - ✓ Implementation of the TSF (ADV\_IMP.2)
  - ✓ Testing: Low-level Design (ATE\_DPT.2)
  - ✓ Flaw Reporting Procedures (ALC\_FLR.2)
  - ✓ Moderately Resistant (AVA\_VLA.3)
  - ✓ Functional Specification (ADV\_FSP\_(EXP).1)
  - ✓ Security-enforcing High-level design (ADV\_HLD\_(EXP).1)
  - ✓ Security-enforcing Low-level design (ADV\_LLD\_(EXP).1)
  - ✓ Architectural Design with Justification (ADV\_ARC\_(EXP).1)
  - ✓ Modular Decomposition (ADV\_INT\_(EXP).1)
  - ✓ Systematic Cryptographic Module Covert Channel Analysis (AVA\_CCA\_(EXP).1)

# High Robustness

- High robustness will build upon Medium robustness requirements and are currently being targeted at the EAL 6 level.
- The exact assurance requirements are still being developed. Completion date is TBD.

# Contact Information

Department of Defense  
ATTN: Jean Schaffer  
9800 Savage Rd  
Fort Meade, Maryland 20755-6740  
[Jhschaf@missi.ncsc.mil](mailto:Jhschaf@missi.ncsc.mil)

Aerospace Corporation  
ATTN: Ken Elliott  
8840 Stanford Blvd, Suite 4400  
Columbia, Maryland 21045  
[elliott@aero.org](mailto:elliott@aero.org)